IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF: CERTAIN ITEMS COLLECTED DURING THE SEARCH OF THE PREMISES KNOWN AS 8861 CHANTILLY WAY, MONTGOMERY, ALABAMA, 36116	2:24mj222 CMR

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, JULE ALBRETSEN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search electronic devices and documents (the "Target Records") collected while conducting a search for electronic devices, specifically mobile phones, at the premises located at 8861 Chantilly Way, Montgomery, Alabama 36116 (the "Premises") on February 9, 2024. The Target Records are currently stored at the FBI office at 5425 W Amelia Earhart Dr, Salt Lake City, Utah, in the District of Utah, as further described in Attachment A. I request authority to seize and search the Target Records as evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1956(a)(2) (money laundering transaction from the U.S. to outside the U.S.), 1956(h) (conspiracy to commit money laundering), 1957 (money laundering transaction exceeding $10,000), and 1960 (unlicensed money transmitting), (collectively, the "Subject Offenses") as more fully set forth below.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I have been employed by the FBI as a Special Agent since November of 2012. I am currently assigned to the FBI Provo Resident Agency. I have investigated a wide variety of federal violations to include complex financial fraud, international kidnapping, bank robberies, threats, felon in possession, and fugitive cases. Virtually all of my investigations include investigating various aspects and use of the Internet and cellular phones. I have completed the SANS Institute Security Essentials course, an in-depth course covering how the Internet functions and discussing Internet related security vulnerabilities, and the CAST Basic Cellular Analysis Training. I have written, reviewed, and executed numerous search warrants. I have participated in investigations that involve sophisticated electronic surveillance methods to include pen registers, trap and trace devices. The facts in this affidavit come from my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1956(a)(2) (money laundering transaction from the U.S. to outside the U.S.) 1956(h) (conspiracy to commit money laundering), 1957 (money laundering transaction exceeding $10,000), and 1960 (unlicensed money transmitting) have been committed by persons known and unknown, including a person named JIMMY CHIEJINE IWEZU.

PROBABLE CAUSE

VICTIMS OF ONLINE ROMANCE SCAMS SEND MONEY TO UTAH SUBJECTS

4. In my training and experience, a romance scam involves a scheme of befriending victims through social networking and convincing them of a romantic interest and then convincing the victim there is an urgent need for money. The scammers, so-called "Yahoo boys," are usually overseas. The romance scam relies upon witting or unwitting accomplices to provide United States bank accounts or addresses to receive the victim's money. They direct their United States accomplices in the United States to move the money after it is received or deposited in their accounts, often to overseas locations. Nigeria is a common destination for funds fraudulently obtained through romance scams.

5. By structuring the transactions through intermediary United States accounts and locations, the perpetrators avoid bank scrutiny. Domestic wire transfers are not scrutinized as closely as international wire transfers. An international wire transfer may trigger inquiry from the bank. When the bank contacts a knowing accomplice to verify whether they really intend to send money to Nigeria, the accomplice confirms the transactions. If the bank contacted the victim to ask the same question, the victim may cancel the transaction, hesitate, or give the bank information that will cause the bank to discover the fraud. In addition, the use of intermediary accounts appears to be calculated to allow the perpetrators to move the funds through several jumps before the victim discovers the fraud and attempts to recall the funds.

6. The primary targets of the scheme and conspiracy under investigation were widowed women above the age of sixty-five. This is so because they are emotionally vulnerable and because they are more likely to have significant savings. The scheme took in millions from its victims. Multiple foreign nationals who were residing in Utah have been charged and

convicted for money laundering the proceeds of this scheme and conspiracy. We obtained warrants to search their electronic devices and reviewed electronic communications on those devices, which are discussed below. These communications, together witness statements, present probable cause to believe Defendant JIMMY IWEZU joined the scheme and conspiracy, opened and provided accounts to be used in the scheme, and conducted transactions in furtherance of the scheme, all in violation of 18 U.S.C. 1341, 1343, 1956, 1957, and 1960.

7. The FBI received a specific complaint regarding a victim with initials C.S., a 75-year old female. She reported that, sometime in February of 2018, she was befriended by an unknown person using the profile "Aaron.Brain" who claimed to be a businessman living in Germany. "Brain" provided photos and discussed his business, claiming he was involved in a business venture supplying pipe for a sewer in Turkey. "Brain" provided photographs of industrial pipes in a warehouse. He told C.S. she could make $600,000 in his business venture. He convinced her to send ten checks totaling $275,000 and five wire transfers totaling $81,000, all between 4/2/2018 and 5/17/2018. She sent the checks and wired the money according to instructions provided by "Aaron Brain," who used online communications. Six of the checks were mailed from outside the District of Utah to individuals located in the District of Utah: Daniel Negedu, Jeffersonking Anyanwu, Onoriode Kenneth Adigbolo, and Chukwudi Kingsley Kalu (together with Richard Ukorebi, David Maduagu, Godsent Nwanganga, and Adriana Sotelo who have been convicted of money laundering conspiracy in Case No. 2:19-cr-190 in the District of Utah, the "Utah Money Transmitters"). Three of the wires were made to an account for JEFFERSONKING ANYANWU's wife. Below are the some of the photographs he provided, and the photograph relating to his business in Turkey. The photographs appear to be manipulated to impose a certain man's head on the body of men in different locations.

8. In connection with the FBI's investigation of romance scams causing funds to be sent to accounts in Utah, the FBI obtained records from numerous financial institutions for accounts belonging to the Utah Money Transmitters, all of whom have been convicted of participating in a money laundering conspiracy. The FBI reviewed statements relating to more than 75 bank accounts at 13 different financial institutions held in these individuals' names for periods ranging from May 2016 through February 2019. There may have been additional accounts held by these individuals or their alter egos during this period.

9. As part of the investigation, the FBI interviewed several of the Utah Money Transmitters. Each admitted that they acted as "pickers" who receive money from Yahoo boys' "clients" (victims) and to transmit them further for a fee. The transactions sometimes involved moving the funds quickly between accounts in the United States. Witnesses identified Adigbolo as a coordinator of the U.S. based pickers. According to witnesses, the typical fee was approximately 15 to 20%, which would be shared among pickers involved in the transaction.

10. In my training and experience, it is a violation of 18 U.S.C. § 1956(h) to conspire to engage in money laundering in violation of 18 U.S.C. § 1957 (knowingly engaging in transactions involving at least $10,000 in criminally derived proceeds). It is also a violation of 18 U.S.C. § 1960 to engage in a money transmitting business without registering the business with FinCEN or obtaining a required state license.

11. A cooperating witness who pleaded guilty to participating in the money laundering conspiracy identified certain of these individuals as Yahoo boys, including Oghenemine Jeffrey Agbroko, Bright Lucas, and Baba G. The same witness identified certain of these individuals as participants in the money laundering, including Jimmy Iwezu, Rukevwe Ologban, and Lori Tsoritse. The communications corroborate these statements.

12. For instance, a series of WhatsApp communications between Adigbolo and "Laju," and between Adigbolo and "Jimmy," reveal their use of electronic devices to engage in transactions and give each other information about the transactions. (Interviewed Utah Money Transmitters identified LORI TSORITSE as "Laju". The phone number associated with "Jimmy" is, according to Apple, a phone number for Jimmy Iwezu, and the full name Jimmy Iwezu appears in the WhatsApp messages when he is requesting payment.)

13. Laju would request that Adigbolo and the Utah Money Transmitters supply accounts and addresses for the Yahoo boys in Nigeria to give to victims. At one point, "Laju" disclosed to Adigbolo, "I get virtually 100k or more every month." Adigbolo and the Utah Money Transmitters would then rely on Jimmy Iwezu, Rukevwe Ologban, and others to provide layers for depositing and transmitting the money to Nigeria.

14. For instance, on March 5, 2019, Laju instructs Adigbolo to "Mail dat cash to rukky." Adigbolo suggests splitting the cash and appears to suggest sending some to Jimmy:

"Oh I b think say na jimmy want am." Laju and Adigbolo then engage in negotiations for the exchange rate, arguing for a rate of 345 vs. 348, Nigerian naira to U.S. dollar. At some point later, Laju confirms, "send to Jimmy," and confirms an exchange rate of 347.

15. On March 6, 2019, Adigbolo tells Laju he sent "Jimmy 60k" and "Rukky 28,380." Throughout these communications, Laju appears to be acting as an intermediary between Adigbolo on one hand and "Jimmy" and "Rukky" on the other. Adigbolo sends Laju screenshots of shipping confirmations for packages sent to the towns where Iwezu and Ologban are located. Laju responds with photographs of cash on a bed. They continue to dispute over the fees and exchange rate. Ultimately, Laju chides Adigbolo for attempting to negotiate a low exchange rate, even after agreeing with the "owner" (in this context, the Yahoo boy) and receiving the money: "i tel d owner say see show am prove he say mk i sell am. after i don promise am 345 350. d same complain jummy complain na rukky complain meanin dem dey rite. jst imagin say I don **lunder** over 200k yanki I never see 200k. he make sens. . . . we dey aid d **lundery** an makin less." The terms I have emboldened appear to be references to the idea that they understood they were engaged in money laundering, or helping with money laundering.

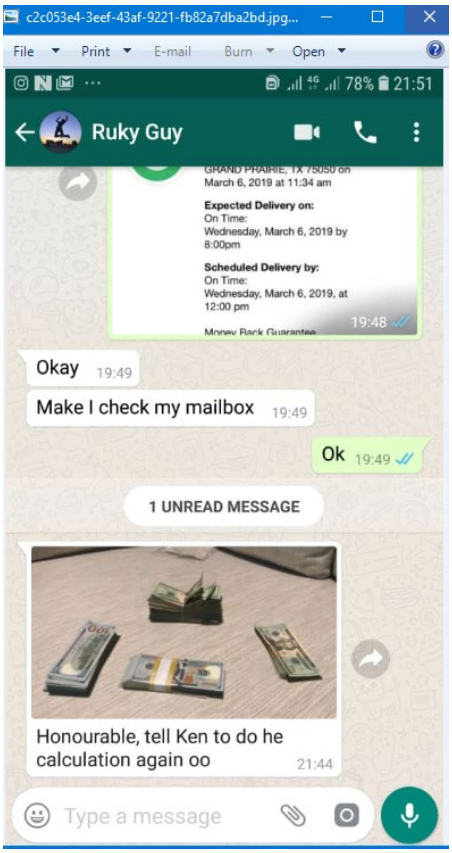
16. "Jimmy" is identified within communications between Adigbolo and Jimmy as Jimmy Iwezu, when he provides Adigbolo his account information.

17. "Rukky" is identified as Rukevwe Ologban in Grand Prairie, Texas in Adigbolo's communications with Laju.

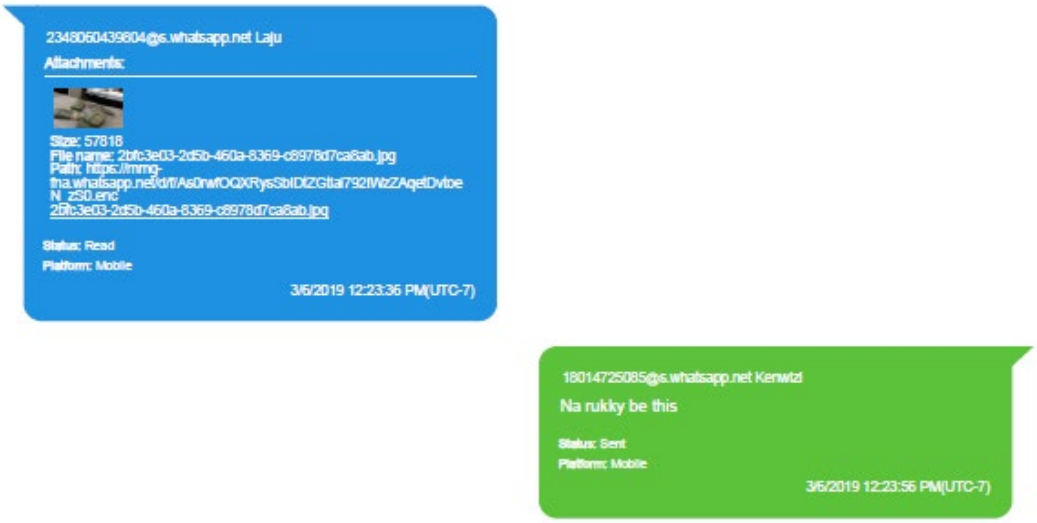
18. In addition to communications with "Laju," it appears Adigbolo communicated directly with "Jimmy," with phone number 1-334-440-4384, reflecting an Alabama area code and phone number. The communications are consistent with those between Adigbolo and Laju, in that they appear to discuss the movement of money. The very first message in the

conversation is from Jimmy: "Confirm correct 60k." He then follows up, "After this transfer is complete am done with this business. Because (1. The Risks involved is much (2. Am not making any reasonable funds out of it)(3. It's great running things with you." After this, on April 25, 2019, there appears to be discussion of working directly together without Laju, and Jimmy expresses concern: "Hope laju nor go vex say I side line himself." Thus, Iwezu's mobile device was used as an instrument in the criminal conduct under investigation and is likely to contain evidence of that conduct similar to the communications just described.

19. We obtained information from Chase bank indicating that Rukevwe Ologban's phone number was 682-230-1795. It does not appear that Ologban and Adigbolo communicated directly. Instead, Laju acted as an intermediary. But Laju occasionally provided screenshots of his WhatsApp communications with Ologban and directed Adigbolo to compensate Ologban through CashApp, a mobile device application for payments. For instance, here are two screenshots Laju sent to Adigbolo through WhatsApp. They appear to show communications between Rukevwe Ologban ("Ruky Guy") and Laju on WhatsApp. They also appear to show that Ologban is using his mobile device to take pictures and screenshots to send to Laju as part of their money transmitting activities:



20. Laju also sends other digital photographs to Adigbolo, which Adigbolo confirms appears to be from Rukevwe Ologban ("Rukky"), presumably because the amount of cash in the photograph was consistent with the amount of cash Adigbolo mailed to Iwezu:



21. The first of the Utah Money Transmitters was arrested on June 4, 2019.

22. The facts above present probable cause to believe these individuals are engaged in a conspiracy to commit violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1956(a)(2) (money laundering transaction from the U.S. to outside the U.S.) 1956(h) (conspiracy to commit money laundering), 1957 (money laundering transaction exceeding $10,000), and 1960 (unlicensed money transmitting).

ARREST OF JIMMY IWEZU AND EXECUTION OF SEARCH WARRANT AT THE PREMISES

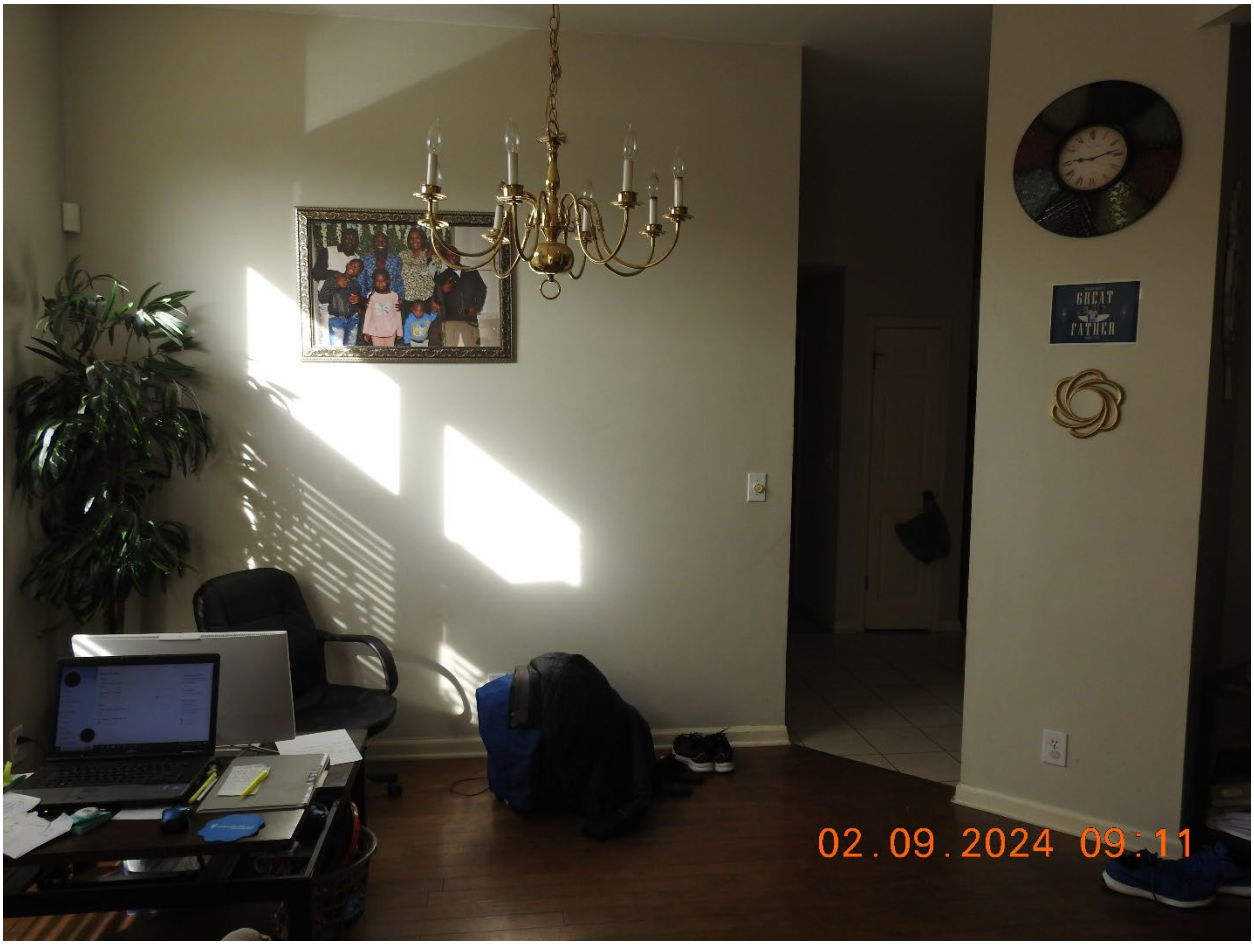
23. On February 9, 2024, prior to the execution of the search warrant, Agents' and TFOs' activated vehicle emergency lights in front of IWEZU's residence, hereafter "the Premises." FBI Task Force Officer (TFO) Keith Pendley used a loudspeaker to make several requests that all occupants exit the Premises. At approximately 9:02 a.m., Jimmy Iwezu exited the Premises. Jimmy Izweu was arrested by Special Agents (SA) Garrett, Barrett, and McLemore

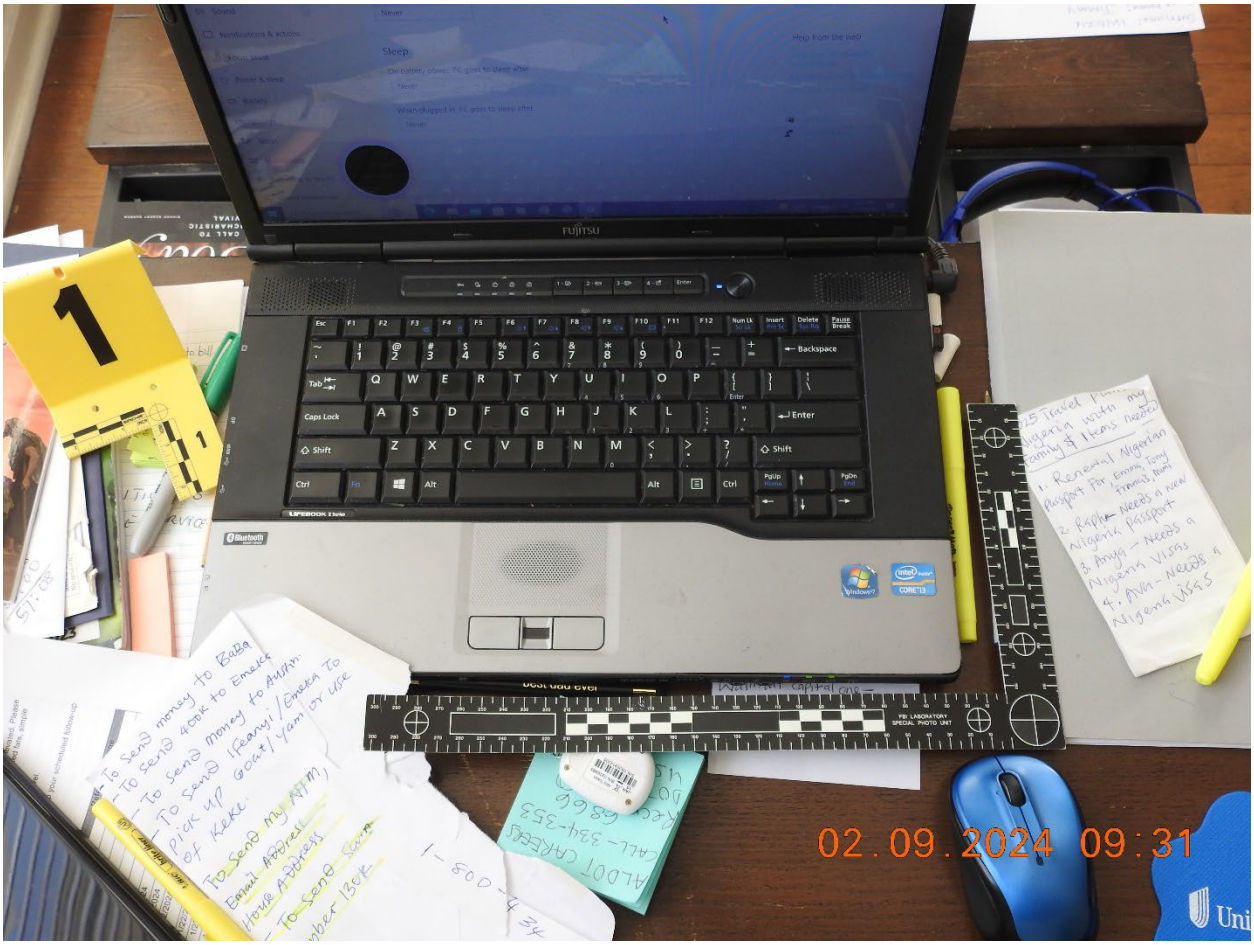
without incident. Once all parties were removed from the residence, Agents entered and cleared the residence. The initial entry of the residence was completed at approximately 9:11 a.m. Law enforcement officers then executed search warrant 2:24-mj-19-JTA issued in the Middle District of Alabama for IWEZU's residence.

24. The items listed in search warrant 2:24-mj-19-JTA to be seized included "mobile phone(s) associated with telephone number 334-440-4384, an Apple iPhone 7, and files found thereon."

25. Search warrant 2:24-mj-19-JTA authorized seizure of "All records found on mobile devices associated with phone number 334-440-4384 relating to violations of 18 U.S.C. §§ 1349 (conspiracy), 1343 (wire fraud), 1956(h) (conspiracy to commit money laundering), 1956(a)(1)(B) (money laundering transactions), 1956(a)(2) (international money laundering transaction), 1957 (money laundering through transaction involving $10,000 or more in criminal proceeds) by JIMMY CHIEJINE IWEZU, occurring after January 1, 2017 to June 4, 2019."

26. It appeared that prior to the arrest, IWEZU was sitting at a small table near the front door in using a laptop and a mobile phone. While clearing the residence, TFO Kyle Sage noticed a laptop and a Samsung Galaxy Note 10 plus on the small table in a powered-on state. After the residence was cleared, TFO Sage changed the power settings of the laptop to remain on due to possible evidence in the volatile memory at approximately 9:05 AM.


GREAT
FATHER
02.09.2024 09:11

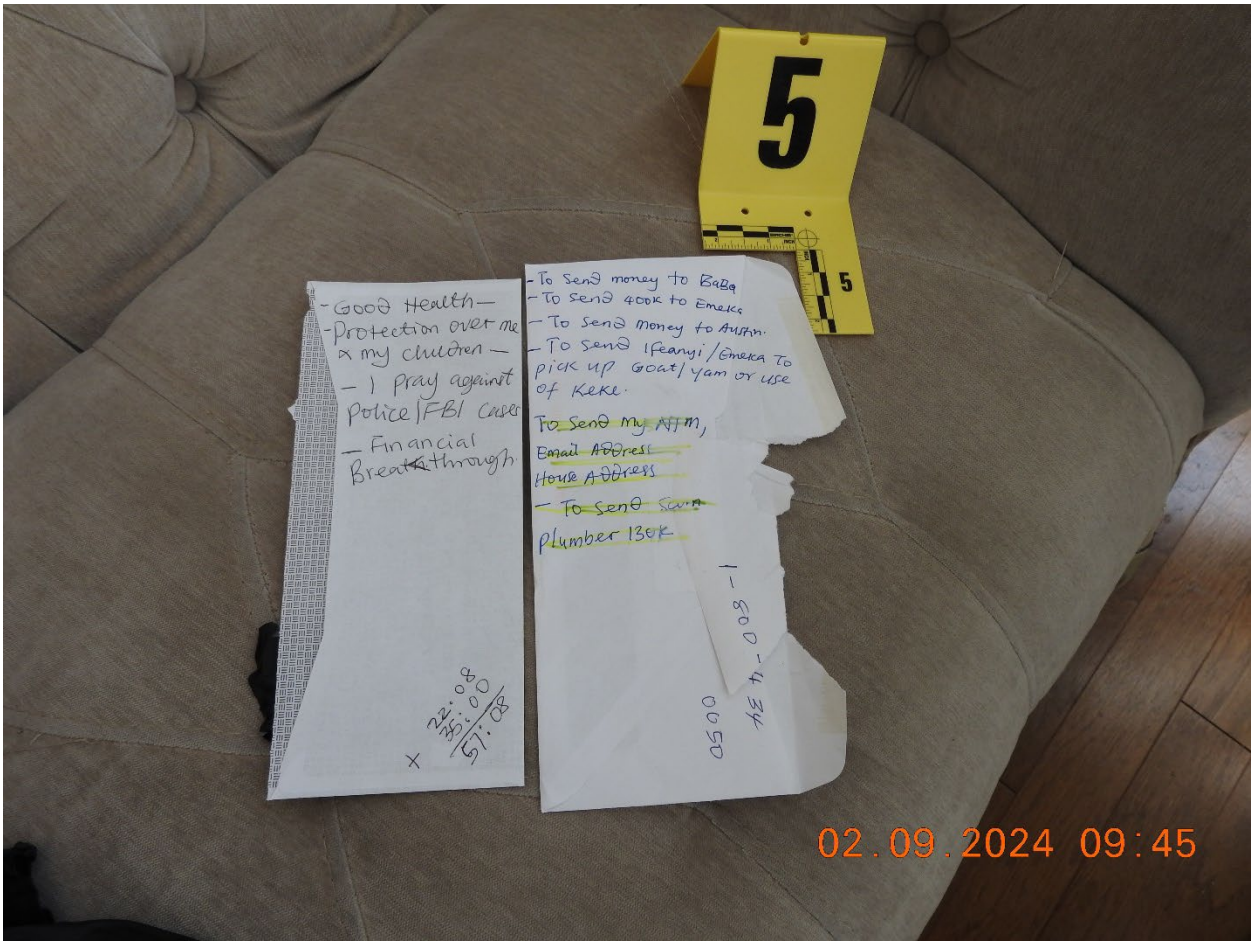


27. In addition to the laptop and the Samsung Galaxy Note 10 plus, there were a number of items on the table observed in plain view including:

a. An envelope with a checklist to send money to a number of individuals including "To send 400k to Emeke"

b. First Bank (a Nigerian bank) RSA Type Token

c. An envelope with notes including "I pray against police/FBI cases"



28. Based on the state of the devices and items on the small table, it seemed likely that IWEZU engaging in online money transfers to or within Nigeria around the time of his arrest.

29. Prior to the arrest of IWEZU, SA Carl Elam learned that the State of Alabama records indicated that IWEZU had not been employed in Alabama since 2016 but has remained a resident of Alabama throughout that period. SA Elam observed that IWEZU was not employed while he was conducting money transfers with Adigbolo, nor did he obtain employment after Adigbolo was arrested on June 4, 2019. Furthermore, IWEZU "worked under" Laju, not Adigbolo. Laju was a major money laundering coordinator based in Nigeria and would not have

been affected by Adigbolo's arrest. Laju's communications with Adigbolo hinted that IWEZU engaged in other money laundering transactions not related to Adigbolo.

30. Given the totality of the circumstances: IWEZU's lack of employment while and after he was laundering money with Adigbolo, his relationship with Laju, and the items observed in plain view during the arrest and clearing of the residence, it appeared that IWEZU likely engaged in violations of 18 U.S.C. 1341, 1343, 1956, 1957, and 1960 after his conduct with Adigbolo.

31. Given that targets of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement and destroy physical records were they to learn of the Government's investigation. Due to the exigent circumstances, SA Elam took steps preserve physical and digital records that were consistent with the types of records they were authorized to seize from electronic mobile devices.

32. Once the residence was cleared, SA Brandon McElmore obtained consent to search from Jimmy Iwezu for the electronic devices. Jimmy Iwezu provided the passcodes for an iPhone 6S (PIN: 200712), Samsung Galaxy Note 10 (PIN: 2023) (both mobile devices were in the scope of the search warrant 2:24-mj-19-JTA), Fujitsu Lifebook laptop (PIN: 1979), and Hewlett Packard All-in-One desktop (PIN: 1979).

33. TFO Sage disabled the screen lock on the Samsung Galaxy Note 10 at approximately 10:05 AM to avoid the device from encrypting its contents. A flash drive with Magnet RAM Capture (version: 1.2.0) software was inserted to a USB port. The random access memory (RAM) was imaged and saved to a sanitized flash drive at approximately 10:15 AM.

The HP desktop was accessed via passcode. The RAM was imaged with the same process at approximately 10:40 AM. The computers were shut down and collected as evidence.

34. While the physical records were not found in mobile devices, they were consistent with the types of records SA Elam and his team were authorized to seize from mobile devices. However, they were located on open surfaces or within containers large enough to store mobile devices. Based upon my and SA Elam's familiarity with the operation of the scheme, we understood that participants used bank accounts and entities to receive and move criminal funds. Accordingly, when SA Elam and his team saw the records while searching containers for mobile devices, they immediately recognized incriminating nature of the records.

35. While searching the residence for mobile devices, the following items and documents were observed, photographed and collected:

Item #	Description	Location
1	Black Fujitsu Laptop with Charger	A
2	Black Android Galaxy Note 10 Plus SM-97SU1	A
3	White HP Desktop	A
4	Apple iPhone 6 Plus A9524	E
5	Money Laundering Documents	A
6	First Bank RSA Type Token	A
7	Money Laundering Documents	A
8	Black Wallet with Financial Cards / Information	E
9	Money Laundering Documents	A
10	Black Wallett	A
11	Black Jansport Backpack	A
12	Document with account information	A
13	Portable SSD	E
14	Money Laundering Documents	E
15	Black bag with four (4) android cell phones inside	E
16	Purple folder with Money Laundering Documents	E
17	HP Gray Chromebook	J
18	Apple iPad in Gray Case	J
19	Gifting donation paperwork	Vehicle
20	Financial Documents	J
21	Financial Documents	G

36. After the execution of the search warrant, the items listed above were transported to the FBI Mobile, Alabama Field Office where they processed in the Evidence Control Room. The items were later shipped to the FBI Salt Lake City, Utah Field Office. They were received into the Salt Lake City Evidence Control Room on March 1, 2024, where they now reside.

37. Specifically, I believe there is probable cause that the above listed items are evidence and fruits or instrumenalities of:

a. Electronic records on computers and storage media in the possession of IWEZU that pertain to the operation of an unlicensed transmitting business (one of the Subject Offenses) that continued even after the original conduct under investigation as outlined in paragraphs 5-22 above.

b. Physical records related to the Subject Offenses that would have been in the scope of search warrant 2:24-mj-19-JTA (in the Middle District of Alabama) if they had been in electronic format on a mobile device.

c. Electronic and physical records related to the Subject Offenses described in search warrant 2:24-mj-19-JTA (in the Middle District of Alabama) that occurred after the time period described in the search warrant.

38. This warrant seeks authorization to retain the items and extracted data collected during the search of IWEZU during the execution of search warrant 2:24-mj-19-JTA on February 9, 2024. Furthermore, it seeks authorization to search the items for evidence of the Subject Offenses.

COMPUTERS AND MOBILE PHONES USED AS INSTRUMENTS OF THE CRIMES AND CONTAIN EVIDENCE OF THE CRIMES

39. As set forth above, the perpetrators used electronic communications platforms to communicate with their victims and each other. Specifically, the perpetrators communicated with each other through WhatsApp, text messages, and other social networking online applications. They also used the mobile devices to take pictures or screenshots of their communications, bank records and transactions, which would be stored on their mobile devices. They also use their mobile devices to take screenshots of communications with one coconspirator to attach to a communication with another coconspirator. They also used money transmitting applications and banking applications, which provide evidence of where the perpetrators have accounts. These pictures too would be stored in the photos on the device as well as in the electronic communications. The mobile devices would contain pictures,

communications, contact lists, applications, and transaction data that constitute evidence of the crimes under investigation.

40. The pictures in Adigbolo's WhatsApp messages, based upon the content of the pictures and the format and layout, suggests that IWEZU used a mobile device in his money transmitting activities to engage in transactions and to create evidence and communications of those activities.

41. In my training and experience, individuals who participate in criminal activity (particularly fraud, drug trafficking, and money laundering) are known to keep two cellular phones, one to conduct personal business and another to conduct illicit business. Individuals participating in international money laundering schemes will have other phones that utilize an international SIM card and/or apps that are capable of voice over IP calls such WhatsApp. Adigbolo's WhatsApp communication with his coconspirators shows there were frequent voice calls made over WhatsApp.

42. In my training and experience, data remains on a computer unless and until it is affirmatively deleted by the user. Even after the user affirmatively deletes the data, the data is merely relegated to "unallocated space" and remains on the computer's drive until it is overwritten.

43. Even if the user had deleted communications from the relevant period, the contact information for the participants in the communications would remain in their devices, as would photographs taken of transactions and communications.

44. In addition, any other devices associated with that number are likely to contain relevant information. This warrant particularly seeks evidence of IWEZU's associations (i.e. contact lists), photographs of cash, receipts, and communications that would be taken with a

phone, as well as electronic communications relating to his activities. In my training and experience, even if a user obtains a new mobile device, data from old devices can easily be ported over into new devices, either through a direct data transfer or by uploading a backup of the old device and downloading the backup to the new device. In my training and experience, it would not be unusual for photographs taken with a mobile device to be imported onto multiple subsequent devices, and for a new device to have photographs and files that are as old as ten years. Information provided by Apple suggests that IWEZU has consistently had an Apple account since 2014.

45. Moreover, more recent communications and transactions involving the unlicensed transmission of criminal proceeds are relevant to establish that transactions with the Utah Money Transmitters were not by mistake or accident. In other words, they are relevant to establish IWEZU knowingly and intentionally engaged in transactions involving criminal proceeds.

46. As described above and in Attachment B, this application seeks permission to search for records that might be found on the computers and mobile devices at the Premises, whatever form they are found in. One form in which the records might be found is data stored on a computer's hard drive or other storage media, including mobile devices. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

47. I anticipate executing these search warrants under the Electronic Communication Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by searching the property identified in Attachment A, respectively and conducting a later search of any data seized or computers found for the information identified in Attachment B.

48. It is anticipated that the search of computers and electronic devices (including without limitation cellular phones or tablets or other electronic communications devices) may include the following:

a. Examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (2) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. Surveying various file directories and the individual files they contain, electronic mail, text messages (or comparable messages in various messaging applications that may be installed on any computer located on the Subject Premises or on the person(s) designated in the search warrant), contact lists, address books, call logs, calendars, notes, appointments, task lists, voice mail, audio files, video files, or pictures, including attachments, to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. Opening or reading portions of electronic mail or text messages (or comparable messages in various messaging applications that may be installed on any

computer located on the Subject Premises or on the person(s) designated in the search warrant)

e. Opening or reading portions of files in order to determine whether their contents fall within the items to be seized as set forth in Attachment B;

f. Scanning storage areas to discover data falling within the list of items to be seized as set forth in Attachment B, to possibly recover any such recently deleted data, and to search for and recover deliberately hidden files falling within the list of items to be seized; and/or

g. Performing key word searches through all computers and electronic storage media (including electronic mail or text messages and attachments thereto stored on such media) to determine whether occurrences of language contained in such storage media exist that are likely to appear in the evidence described in Attachment B.

CONCLUSION

49. Based on the forgoing, I request that the Court issue the proposed search warrants.

Respectfully submitted,

Jule Albretsen

JULE ALBRETSEN
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Subscribed and sworn to before me on 3/7/2024, 2024

Cecilia M. Romero

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

A. Items, and their respective data extractions, that were collected during the execution of search warrant 2:24-mj-19-JTA on February 9, 2024 at the residential property located at 8861 Chantilly Way, Montgomery Alabama 36116. The items and data are currently located at the FBI Salt Lake City Field Office in Salt Lake City, Utah:

Item #	Description	Location
1	Black Fujitsu Laptop with Charger	A
2	Black Android Galaxy Note 10 Plus SM-97SU1	A
3	White HP Desktop	A
4	Apple iPhone 6 Plus A9524	E
5	Money Laundering Documents	A
6	First Bank RSA Type Token	A
7	Money Laundering Documents	A
8	Black Wallet with Financial Cards / Information	E
9	Money Laundering Documents	A
10	Black Wallett	A
11	Black Jansport Backpack	A
12	Document with account information	A
13	Portable SSD	E
14	Money Laundering Documents	E
15	Black bag with four (4) android cell phones inside	E
16	Purple folder with Money Laundering Documents	E
17	HP Gray Chromebook	J
18	Apple iPad in Gray Case	J
19	Gifting donation paperwork	Vehicle
20	Financial Documents	J
21	Financial Documents	G

ATTACHMENT B

Property to be seized

The Property to be seized includes all records relating to violations of 18 U.S.C. §§ 1343 (wire fraud), 1956(h) (conspiracy to commit money laundering), 1956(a)(1)(B) (money laundering transactions), 1956(a)(2) (international money laundering transaction), 1957 (money laundering through transaction involving $10,000 or more in criminal proceeds) and 1960 (unlicensed money transmitting business) by JIMMY CHIEJINE IWEZU those violations occurring from January 1, 2017 to the present and those violations involving romance scams or similar online scams or the proceeds of such scams, including:

a. Records and information relating to IWEZU transmitting funds on behalf of others within the United States or from the United States to a place outside the United States, whether directly, indirectly, or by exchange;

b. Records and information relating to IWEZU's fees and rates for transmitting funds on behalf of others;

c. Records and information relating to Treynor Soft, Truine Resources or Triune Resources, Bluewall, or IWEZU's use of other entities to transmit money on behalf of others within the United States or from the United States to Nigeria, whether directly, indirectly, or by exchange;

d. Records and information relating to IWEZU's knowledge of the source of funds for the transmissions she engage in, including records outside the Relevant Period that may indicate a lack of mistake for criminal proceeds transmitted during the Relevant Period;

e. Records and information relating to financial accounts controlled by IWEZU or his associates at banks or credit unions from the beginning of the Relevant Period to the present;

f. Records and information relating to efforts to circumvent money laundering controls at Ping Express for Onoriode Kenneth Adigbolo, Richard Ukorebi, Chukwudi Kingsley Kalu, Jeffersonking Anyanwu, Daniel Negedu, or David Maduagu, Godsent Nwangaga, Adriana Sotelo or their associates;

g. Records and information relating to communications with Onoriode Kenneth Adigbolo, Richard Ukorebi, Chukwudi Kingsley Kalu, Jeffersonking

Anyanwu, Daniel Negedu, or David Maduagu, Godsent Nwangaga, Adriana Sotelo or their associates;

h. Records and information establishing IWEZU's sources of income other than transmitting transmission of funds on behalf of others during the Relevant Period;

i. Lists of IWEZU's contacts;

j. For each computer or storage device (either, a "COMPUTER"):

(i) evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

(ii) evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

(iii) evidence of the lack of such malicious software;

(iv) evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

(v) evidence indicating the computer user's state of mind as it relates to the crime under investigation;

(vi) evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

(vii) evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

(viii) evidence of the times the COMPUTER was used;

(ix) passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

(x) documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

(xi) records of or information about Internet Protocol addresses used by the COMPUTER;

(xii) records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

(xiii) contextual information necessary to understand the evidence described in this attachment.